## REMARKS

Reconsideration of this application is respectfully requested in view of the foregoing amendment and the following remarks.

By the foregoing amendment, claims 1 and 6 have been amended and claim 5 canceled. Thus, claims 1-4 and 6-8 are currently pending in the application and subject to examination.

### I. Specification

The Office Action mailed May 15, 2007 objects to the specification as failing to provide proper antecedent basis for the computer software storage medium because applicant has failed to define the computer software storage medium. The Applicant submits that computer software storage medium is a term commonly used in the art, and one of ordinary skill in the art would not require additional definition in order to understand the meaning of the term.

### II. 35 U.S.C. § 101

The Office Action rejects claim 6 under 35 U.S.C. § 101 as being directed to nonstatutory subject matter. Claim 6 has been amended responsive to this rejection. Amended claim 6 is directed to a computer system including an anti-virus application installed on a network server. Thus, the Applicants submit that claim 6 is directed to statutory subject matter.

The Office Action rejects claim 7 under 35 U.S.C. § 101 as being directed to nonstatutory subject matter because "computer software storage medium" has not been defined in the specification. As discussed above, the Applicants submit that this is a commonly known term in the art and is being used according to its customary usage.

See U.S. Patent No. 5,966,143 at column 6, lines 39-column 7, line 3; U.S. Patent No. 6,457,171 at column 3, lines 32-61; and U.S. Patent No. 6,606,694 at column 3, lines 1-31. For clarity, the specification is herein amended to incorporate these patents by reference under MPEP § 2163.07.

## III. 35 U.S.C. § 103

Claims 1-7 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,757,830 to Tarbotten et al. ("Tarbotten") in view of U.S. Pub. No. 2003/0088680 to Nachenberg et al. ("Nachenberg"). It is noted that claims 1 and 6 have been amended and claim 5 has been canceled. To the extent that the rejection remains applicable to the claims currently pending, the Applicant hereby traverses the rejection as follows.

### A. Claims 1-4

Applicant's invention as now set forth in claim 1 is directed to a method of preventing the infection of a computer network by a computer virus, where that virus can spread by e-mail traffic, the method including in the event that a new virus is detected by a provider of the anti-virus application, sending a notification of this event from the provider to the anti-virus application, at the anti-virus application, responding to said notification by discontinuing normal handling of e-mails, wherein discontinuing normal handling of e-mails includes failing to deliver incoming e-mails or their attachments to their recipients within the network and causing these e-mails or attachments to be re-directed to a buffer for safe storage; subsequently generating a signature for the virus at the anti-virus application provider and providing that signature to the application at the gateway; at the gateway, after receiving the signature, using the

application to scan the previously buffered e-mails or attachments for the virus, after scanning the buffered e-mails, delivering e-mails or attachments which are virus free to their recipients; and causing the normal handling of e-mails at the e-mail gateway to be resumed.

This provides an anti-virus application configured to prevent a virus infection beginning at the detection of a new virus. Rather than waiting until a signature for a newly detected virus is identified, the present invention discontinues normal service immediately upon notification of detection of a new virus and re-directs all e-mails to a buffer for safe storage. Once a signature is provided to the application, the present invention scans the buffered e-mails and transmits virus free e-mails before returning to normal handling of e-mails. This provides a stop gap measure to protect networks while a signature is being developed.

In contrast, both Tarbotten and Nachenburg relate to conventional virus scanning systems where signature and other detection schemes are provided at a gateway, and e-mails are intercepted if they match any of the signatures or other defined rules. Tarbotten and Nachenburg do not disclose a system that blocks infected e-mails when no signature for a newly released virus is available, even though the anti-virus provider is aware of the virus.

Tarbotten teaches a system that determines a mail latency delay, stores the mail for the latency period, and the rescans the mail with the latest virus definitions and other parameters. See Tarbotten Figure 3. However, Tarbotten applies a latency delay to e-mail based on identified characteristics of the e-mail rather than diverting all e-mail based on notification of a new virus from the provider. (See column 6, lines 59-67). In

contrast, the present invention **discontinues normal handling of e-mail in response to notification of the detection of a new virus**, causes incoming e-mails or attachments to be re-directed to a buffer for safe storage; and **after receiving the signature, scans the previously buffered e-mails or attachments**, and **causes the normal handling of e-mails at the e-mail gateway to be resumed**.

Nachenburg fails to cure the deficiency in Tarbotten.

For at least this combination of reasons, the Applicant submits that claim 1, as amended, is allowable over the cited art. As claim 1 is allowable, the Applicant submits that claims 2-4, which depend from allowable claim 1, are therefore also allowable for at least the above noted reasons and for the additional subject matter recited therein.

B. Claims 6 and 7

The Applicants submit that Tarbotten and Nachenburg, whether taken alone or in combination, do not disclose a computer system or a computer software storage medium having stored thereon an antivirus application arranged to receive a **notification from the provider . . . which notification causes the application to prevent delivery of e-mails or attachments received at the gateway and to divert these e-mails to a buffer** and arranged to **subsequently receive a second notification from the provider which notification causes the application to cease preventing delivery of newly received e-mails**, as recited in claims 6 and 7.

The inventions recited in claims 6 and 7 involve a first notification sent by the provider that diverts the flow of e-mail to a buffer and a second notification that causes the gateway to resume normal delivery of e-mail.

In contrast, Tarbotten and Nachenburg merely scan e-mails or attachments based on distributed signatures. These types of systems rely on the distribution of a signature to occur quickly enough to prevent damage, whereas the invention recited in claim 7 diverts e-mails to a buffer upon receipt of a first notification and does not cease preventing delivery of e-mails until the subsequent receipt of a second notification.

For at least this combination of reasons, the Applicants submit that claims 6 and 7 are allowable over the cited art.

C. Claim 8

Applicant's invention as set forth in claim 8 is directed to a method of preventing the infection of a computer network by a computer virus, the method comprising in the event that a new virus is detected by the provider of the anti-virus application, calculating a checksum for the file carrying the virus or a relevant part of that file, and sending a notification containing the checksum from the provider to the anti-virus application, and at the anti-virus application, using the checksum to screen e-mails and/or their attachments for the virus until such time as a signature for the virus is received by the e-mail gateway from the application provider.

Tarbotten teaches an e-mail message including a header portion including a checksum value for the e-mail message as a whole as a countermeasure against attempts to falsely insert data indicating that a minimum delay period has already been applied to the message.

Tarbotten does not disclose or suggest using a checksum to screen e-mails for a virus, as recited in claim 8. Additionally, Tarbotten does not teach a checksum provided by the anti-virus application provider, as recited in claim 8. Furthermore, Tarbotten

does not disclose or suggest replacing the use of the checksum from the anti-virus application provider with a signature for a virus when a signature is received from the application provider.

Nachenburg fails to cure the deficiency in Tarbotten.

For at least this combination of reasons, the Applicants submits that claim 8 is allowable over the cited art.

## CONCLUSION

For all of the above reasons, it is respectfully submitted that the claims now pending patentability distinguish the present invention from the cited references. Accordingly, reconsideration and withdrawal of the outstanding rejections and an issuance of a Notice of Allowance are earnestly solicited.

Should the Examiner determine that any further action is necessary to place this application into condition for allowance, the Examiner is encouraged to telephone the undersigned representative at the number listed below.

In the event this paper is not considered to be timely filed, the Applicants hereby petition for an appropriate extension of time. The fee for this extension may be charged to our Deposit Account No. 01-2300. The Commissioner is hereby authorized to charge any fee deficiency or credit any overpayment associated with this communication to Deposit Account No. 01-2300 with reference to Attorney Docket No. 108347-00031.

Respectfully submitted,

Arent Fox LLP

Sheree T. Rowe
Attorney for Applicants
Registration No. 59,068

**Customer No. 004372**
1050 Connecticut Ave., N.W.
Suite 400
Washington, D.C. 20036-5339
Telephone No. (202) 715-8492
Facsimile No. (202) 857-6395